

0000 公司

人力資源安全管理作業程序

ISMS-B-004

版本 1.0

中華民國 105 年 MM 月 DD 日

文件編號	ISMS-B-004	人力資源安全管理作業程序	文件類別	限閱
版次	V1.0		發布日期	105/MM/DD

1. 目的.....1

2. 範圍.....1

3. 權責.....1

4. 定義.....1

5. 作業內容.....1

6. 相關資料.....4

7. 附件.....4

文件編號	ISMS-B-004	人力資源安全管理作業程序	文件類別	限閱
版 次	V1.0		發布日期	105/MM/DD

## 1. 目的

OO 公司(以下簡稱本公司)為建立適當的控制以減少因人為過失、偷竊、詐欺、濫用或誤用資訊處理設備所造成的資訊安全風險，確保所有資訊使用者，了解其資訊安全管理相關責任，正確的執行其職務，並進行相關教育訓練以降低人為錯誤的風險。

## 2. 範圍

用於本公司所有員工，承包商及第三方人員皆需遵守。

## 3. 權責

### 3.1 資訊安全委員會

核定資訊安全教育訓練計畫。

### 3.2 資訊安全推動組

3.2.1 負責資訊安全教育訓練計畫擬定與執行。

3.2.2 備妥相關資訊安全文件，以利人員並瞭解資訊安全相關規定。

### 3.3 人事單位

負責本公司人力資源管理行政作業。

## 4. 定義

### 4.1 內部人員

包含編制內正式聘任員工、約用人員、非正式員工、派遣員工、臨時員工（約聘人員、工讀生）。

### 4.2 人力派遣或委外人員

因業務需要，長時間派駐在本公司辦公區域及機房區域活動之外部人員。

### 4.3 訪客

因業務需要，短時間在本公司辦公區域及機房區域活動之人員。

## 5. 作業內容

5.1 應針對本公司各單位所需各職務（位）之工作要求，建立職位角色或職務責任之定義。

### 5.2 員工晉用與篩選

5.2.1 對於新進員工，及員工晉用、任用，應依招募作業辦法之相關規定辦理。

5.2.2 當員工約聘僱條件或契約有所變更時，應呈報權責主管核示。

5.2.3 員工晉用與篩選，均詳查員工學歷、工作資格、作業技能及

文件編號	ISMS-B-004	人力資源安全管理作業程序	文件類別	限閱
版次	V1.0		發布日期	105/MM/DD

身份證明文件等背景資訊並考量公司職務作業需求及法令、法規之要求，用人單位需依據查核並備妥任用之相關文件。

5.2.4 權責主管對任用職務具有存取敏感資料(如存取關鍵服務、客戶資訊及客戶要求的內容)之員工，應採取必要之管制措施，並覆核其權限之適切性。

5.2.5 權責主管對可存取機密性、敏感性資訊或系統之員工，及因工作需要須配賦系統存取特別權限之員工，應加強評估及考核。

5.2.6 對於本公司所任用之內部及委外人員報到時，應閱讀相關資訊安全文件與要求，並充分瞭解資訊安全之工作責任與要求，並簽署保密切結書。

5.2.7 各項業務，必須指定專責之負責人及代理人，於業務負責期間擔負或代理業務之管理工作，並配合資訊安全政策之要求，進行安全管理。本公司資訊安全推動組資訊安全職責詳見「資訊安全工作執掌表」。

### 5.3 責任釐清與安全事項說明

5.3.1 人力資源單位應依據「資訊安全政策」規範，告知員工對本公司資訊安全應負的法律責任與權利。

5.3.2 員工於服務期間皆應遵守本公司管理之相關規定，因業務所獲知之機密資訊及敏感資料(如存取關鍵服務資料、客戶資料及客戶要求的內容資料等)，非經權責主管授權不得對外透露。

### 5.4 人力資源安全事項

5.4.1 正式員工、派遣人員、臨時員工（約聘人員、工讀生）、第三方派駐本公司人員，在進入本公司服務時，都應簽署保密合約書並遵守本公司資訊安全規範。

5.4.2 應告知所有員工軟體之使用須遵循智慧財產權規定，包括不使用非法取得之軟體或利用網路下載的不明軟體。

5.4.3 各單位委外案件應將保密條款列入合約條款之一，並約定違反保密條款之罰則。

5.4.4 員工離職時，應備妥離職申請書及離職手續辦理清單，辦理各項離職相關事宜，包括終止該人員之存取權限，及清除或停用該人員使用相關系統帳號，並辦理資訊資產之歸還作業，若為可接觸機密性、敏感性資料員工離職時，應立即取消其電腦帳號或更換密碼。

5.4.5 員工於關係企業間轉調，應依關係企業員工轉調之規定辦理關係企業間轉調相關事宜；員工內部轉調至其他單位，應備

文件編號	ISMS-B-004	人力資源安全管理作業程序	文件類別	限閱
版次	V1.0		發布日期	105/MM/DD

妥人員異動申請單，辦理內部轉調相關事宜。

5.4.6 員工離職或調動或職務變動時，應由人力資源單位會知各單位系統管理或系統帳號管理人員，刪除原有系統帳號或申請新系統使用帳號，請依【存取控制管理作業程序】辦理。

5.4.7 對所經辦之機密性或敏感性資料之管控與收存，應遵守保密合約書文件之規定。員工於離職後，對於工作上所獲知之機密性與敏感性資料，亦應遵守保密合約書文件之規定，不得任意洩露；人力資源單位應於員工離職作業中再次提示要求遵守作業程序保密合約書文件之規定。

5.4.8 員工離（調）職時，需將原職務所擁有及使用之資訊資產辦理移交或歸還手續。

5.4.9 委外人員離（調）職或合約終止時，應歸還於執行業務期間所擁有或使用之屬於本公司的資訊資產，並根據保密切結書之要求持續負有資訊保密之責任。

5.4.10 委外廠商駐點服務人員完成任務或離職時，需通知委外權責單位，並應辦妥移交手續，繳回其所使用之資料、證件、設備與軟體，並且取消其提供服務所需各項作業權限。

5.4.11 資訊資產歸還時，應依據【實體與環境安全管理作業程序】過濾或清除所包含之資訊，避免因資訊資產報廢或再利用而使敏感資訊外洩。

## 5.5 資訊安全事件通報

所有人員發現資訊安全事件，應依據「資訊安全事故管理作業程序」進行通報，以確保事件發生時有適當之處理。

5.6 員工、訪客及委外人員進出本公司辦公區域及機房，依據【實體與環境安全管理作業程序】辦理。

## 5.7 教育訓練

5.7.1 資訊安全推動組應制訂「**資訊安全年度資訊安全教育訓練計畫表**」，定期進行資訊安全教育訓練，以提高本公司內部及委外人員之資訊安全意識，並使其遵守資訊安全規定。

5.7.2 為建立員工正確認知資訊安全、提升資訊安全水準，應規劃每年辦理資訊安全教育訓練，其中主管、資訊技術人員、業務人員及一般人員，每年至少須分別達到 3、12、6、3 小時之資訊安全教育訓練，

5.7.3 資訊安全教育訓練內容之安排，應依之內部及委外人員工作角色及業務內容為基礎，並以適當方式評估訓練成果。

5.7.4 資訊安全工作分組彙總本公司資訊安全及提昇員工之專業技能教育訓練，提供予資訊發展暨安全管理委員會核定後，據以執行。

文件編號	ISMS-B-004	人力資源安全管理作業程序	文件類別	限閱
版次	V1.0		發布日期	105/MM/DD

5.7.5 資訊安全工作分組應利用內部系統，隨時對本公司員工公告資訊安全宣導事項，以提升員工資訊安全意識，必要時應將相關規範通告委外人員。

#### 5.8 保密合約書及委外保密切結書之維護

5.8.1 資訊安全推動組依據「**遵循性管理作業程序**」辦理保密切結書或保密合約書之審視維護事宜。

5.8.2 審視作業應特別著重存取資訊之機敏性內容，如時間、日期、資訊內容、通訊內容及使用者之個人資料及隱私等保護要求。

#### 5.9 懲戒規定

內部及委外人員於任職或執行委託業務期間，應遵守本公司資訊安全相關規定，若違反資安相關規定(如洩密、盜取個人資料…等)，將依依相關法令、本公司相關規定及契約懲處。

### 6. 相關資料

- 6.1 【資訊安全組織管理作業程序】
- 6.2 【資訊安全政策】
- 6.3 【實體與環境安全管理作業程序】
- 6.4 【存取控制管理作業程序】
- 6.5 【**遵循性管理作業程序**】

### 7. 附件

- 7.1 **資訊安全年度教育訓練課程計畫表**